JOURNAL OF COMBINATORIAL THEORY (A) 15, 45–53 (1973)

On Maximal t-Linearly Independent Sets

BODH RAJ GULATI

Department of Mathematics, Southern Connecticut State College, New Haven, Connecticut 06515

AND

BRUCE MCK. JOHNSON AND UWE KOEHN

University of Connecticut, Storrs, Connecticut 06268

Communicated by B. Segre

Received August 24, 1971

Consider a finite $t + r - 1$ dimensional projective space PG$(t + r - 1, s)$ over a Galois field GF(s) of order $s = q^h$, where q and h are positive integers and q is the prime characteristic of the field. A collection of k points in PG $(t + r - 1, s)$ constitutes an $L(t, k)$-set if no t of them are linearly dependent. An $L(t, k)$-set is maximal if there exists no other $L(t, k')$-set with $k' > k$. The largest k for which an $L(t, k)$-set exists is denoted by $M_t(t + r, s)$. K. A. Bush [3] established that $M_t(t, s) = t + 1$ for $t \geqslant s$. The purpose of this paper is to generalize this result and study $M_t(t + r, s)$ for t, r, and s in certain relationships.

1. INTRODUCTION

The problem of constructing fractional replicates of the s^m designs, where s is a prime power, is not new in the literature. However, so far as the subject matter of this paper is concerned, the contributions made by Bose [1, 2], Fisher [4, 5], Segre [8, 9, 10], Tallini [11] and recently by Gulati and Kounias [6] are of interest. The basic concept remains the same as in Bose [1] inasmuch as the maximum number of factors in a symmetrical factorial design in which each factor operates at s levels, blocks are of size s^{t+r}, and no main effects or t-factor $(t > 1)$ or lower order interaction is confounded with blocks, is given by the maximum number of distinct points in finite projective space $PG(t + r - 1, s)$ based on $GF(s)$ so that no t points among them lie on a $(t - 2)$-flat.

In an elegant paper, Bose [2] established that, for a fractionally re-

plicated design $(1/s^d) \times s^k$, consisting of a single block with s^{t+r} plots, $t + r = k - d$, the maximum possible value of k is $M_{2u}(2u + r, s)$ if no u-factor or lower order interaction is aliased with another u-factor or lower order interaction. In case no u-factor is to be aliased with a $(u + 1)$-factor or lower order interaction, then the maximum value of k is given by $M_{2u+1}(2u + r + 1, s)$. For given k and u, we need to maximize d, that is, take as high a fraction of the full factorial design as possible.

The number $M_t(t + r, s)$ also plays a significant role in the information theory. If there is a channel capable of transmitting s distinct symbols, then, for a group code (k, d) with d information symbols and fixed redundancy $k - d$, the maximum value of k for which u errors can be corrected with certainty is $M_{2u}(2u + r, s)$. Similarly, the maximum value of k for which u errors can be corrected with certainty and $u + 1$ errors detected is given by $M_{2u+1}(2u + r + 1, s)$. This interconnection between the theory of confounding and fractional replication developed by Fisher, Finney, Bose, and Kishan and theory of error correcting codes due to Hamming and Slepian has been elegantly brought out by Bose [2].

Thus, the problem of finding the maximum value, $M_t(t + r, s)$ and of obtaining the maximal sets in $PG(t + r - 1, s)$ has gained importance. In the absence of a complete solution, sharp bounds are desirable. Through the works of several pioneers including Barlotti, Bose, Seiden, Segre, Tallini, Quist, and many other research workers, the study of ovals in finite projective planes over a finite field, $M_3(3 + r, s)$, may already have reached a saturation point (a complete list of the values and bounds in historical order is given in Segre [10]), the investigation for $t \geqslant 4$ has scarcely begun. In this paper, we shall restrict ourselves to an extension of Bush's result. The remaining results are of the same spirit for the cases $s = 2$ and $s = 4$ based on fields of characteristic two.

Segre [8, 9] showed that for s odd

$$M_3(3, s) = s + 1, \qquad s > 3, \tag{1.1}$$

$$M_4(4, s) = s + 1, \qquad s > 4, \tag{1.2}$$

$$M_5(5, s) = s + 1, \qquad s > 5. \tag{1.3}$$

For any n in $PG(n, s)$, a normal rational curve is a $(s + 1)$-arc or $L(t, s + 1)$-set. For $n = 2, 3$, the converse is true, i.e., an $L(t, s + 1)$-set in $PG(2, s)$ is a conic, an $L(t, s + 1)$-set in $PG(3, s)$ is a twisted cubic. The latter result is proved by projection from a point of the cubic onto a plane.

Gulati and Kounias [6] established that for $s = 2^h$, $h > 2$,

$$M_4(4, s) = s + 1, \qquad \text{for} \quad s > 4. \tag{1.4}$$

In an unpublished thesis, Gulati [7] established that

$$M_{t+1}(n+2, s) \leqslant 1 + M_t(n+1, s), \qquad \text{for} \quad n \geqslant t-1. \tag{1.5}$$

Thus, one can easily show that for $s = 2^h$, $h > 2$,

$$s + 1 \leqslant M_5(5, s) \leqslant s + 2. \tag{1.6}$$

2. Results

THEOREM 1. *$M_t(t + r, s) = t + r + 1$ for $t \geqslant s(r+1)$ and*
$\geqslant t + r + 2$ for $t < s(r+1)$.

Proof. Plainly, if $L(t, k)$ is maximal, then $k \geqslant t + r$. In fact, we may suppose that the set contains $(t + r)$-linearly independent points. Further, by suitable choice of basis we may suppose E_i, $i = 1, 2, \ldots, t + r$, to be in the set, where E_i has a one in position i and zeros elsewhere. If the set contains any other additional point, it is clear that it must have at least t non-zero coordinates. Further, if it contains two additional points, then any linear combination of the two must have at least $t - 1$ non-zero coordinates. Let A_1 and A_2 be two points. Then, up to multiples, the possibilities for the corresponding coordinates of A_1 and A_2 are:

	x_1	x_2	x_3	x_4	x_4	$\cdots$	x_s	x_{s+1}
A_1:	1	0	1	1	1	$\cdots$	1	1
A_2:	0	1	1	α	α^2	$\cdots$	α^{s-3}	α^{s-2}

(2.1)

α being a primitive element of $GF(s)$. The case in which both coordinates are zero is of no interest. Let X_j be the number of times the j-th of the above possibilities, or a multiple thereof, appears in A_1, A_2. Then

$$X_j \leqslant \begin{cases} r, & j = 1, 2, \\ r + 1, & j > 2. \end{cases} \tag{2.2}$$

Adding these inequalities,

$$\sum_{j=1}^{s+1} X_j \leqslant (s-1)(r+1) + 2r. \tag{2.3}$$

As we may suppose A_1 and A_2 do not have corresponding coordinates which are both zero, $X_1 + \cdots + X_{s+1} = t + r$. Thus

$$t \leqslant s(r+1) - 1. \tag{2.4}$$

Accordingly, the inequalities (2.2) cannot be satisfied if $t \geqslant s(r+1)$. Plainly, a maximal set must contain at least $t + r + 1$ points. The first

assertion is established. If $t < s(r+1)$, then there are obviously non-negative integer X_j's satisfying (2.2) with $X_1 + \cdots + X_{s+1} = t + r$.

COROLLARY. *For* $r > 1$, $M_t(t+r, s) \leqslant t + r + s$ *for* $sr \leqslant t < s(r+1)$.

Proof. From Theorem 1,

$$M_t(t+r-2, s) = t + r - 1, \quad \text{for} \quad t \geqslant s(r-1), \tag{2.5}$$

$$M_t(t+r-1, s) = t + r, \quad \text{for} \quad t \geqslant sr. \tag{2.6}$$

Suppose an $L(t, k)$-set is maximal. Select from the set $t + r - 2$ points which span a $(t + r - 3)$-dimensional projective space. From (2.5) at most one additional point from the set lies in this space. Further, it is well known that $s + 1$ $(t + r - 2)$-dimensional spaces pass through the $(t + r - 3)$-dimensional space. From (2.6) each of these contains at most one additional point from the set. ∎

The idea used in the proof of Theorem 1 may be used to examine the possibility of adjoining three or more points to the E_i's. The problem is, however, somewhat more complicated and our results are fragmentary. In the interest of brevity, we pursue the problem in the cases of $s = 2$ and 4.

THEOREM 2. For $t > 3$,

$$M_t(t+r, 2) = t + r + 2, \text{ for } f_2(r) \leqslant t \leqslant 2r + 1, \text{ and}$$
$$\geqslant t + r + 3, \text{ for } t < f_2(r),$$

where

$$f_2(r) = \begin{cases} (r+2) + \left[\frac{r+2}{3}\right], & \text{for} \quad r = 0, 1 \bmod 3, \\ (r+1) + \left[\frac{r+2}{3}\right], & \text{for} \quad r = 2, \bmod 3, \end{cases} \tag{2.7}$$

where $[y]$ *is the integer part of* y.

Proof. From Theorem 1, $M_t(t+r, 2) \geqslant t + r + 2$ for $t \leqslant 2r + 1$. Suppose a maximal set contains the $t + r$ E_i's and three additional points A_1, A_2, and A_3. The possibilities for the corresponding coordinates of the A's, up to multiples, are

(2.8)

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
A_1:	0	0	1	1	0	1	1
A_2:	0	1	0	1	1	0	1
A_3:	1	0	0	0	1	1	1

Any strict combination of u, $u = 1, 2, 3$ of the A's can have at most $r + u - 1$ zero coordinates. Defining the X_j's as above and considering all combinations yields

$$BX \leqslant D, \tag{2.9}$$

where

$$B = \left[\begin{array}{c|ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}\right], \qquad D = \left[\begin{array}{c} r \\ r \\ r+1 \\ \hline r+1 \\ r+1 \\ r+2 \\ \hline r \end{array}\right],$$

and

$$X' = (X_1, X_2, \ldots, X_7).$$

Summing all the inequalities yields

$$\sum_{j=1}^{7} X_j \leqslant (2r + 1) + \left[\frac{r+2}{3}\right] = \begin{cases} 7p + 1, & \text{if } r = 0 \bmod 3, \\ 7p + 4, & \text{if } r = 1 \bmod 3, \\ 7p + 6, & \text{if } r = 2 \bmod 3. \end{cases} \tag{2.10}$$

Summing only the inequalities in which X_j appears yields

$$2X_j + \sum_{i=1}^{7} X_i \leqslant \begin{cases} 3r + 1, & j = 1, 2, 3, \\ 3r + 3, & \text{otherwise.} \end{cases} \tag{2.11}$$

The inequalities (2.10) give upper bounds on the values of t for which a maximal set may contain three A's. In general, these bounds are not sharp and the three cases must be considered individually:

$r = 3p$

The maximum value of $\sum_{j=1}^{j=7} X_j = 7p + 1$ is attained for

$$X_j = \begin{cases} p, & j = 1, 2, 3, 4, 5, 6, \\ p + 1, & j = 7. \end{cases}$$

$r = 3p + 1$

The upper bound (2.10) is sharp. A solution is given by

$$X_j = \begin{cases} p, & j = 1, 2, 3, \\ p + 1, & j > 3. \end{cases}$$

$r = 3p + 2$

Suppose that $t + r = X_1 + X_2 + \cdots + X_7 = 7p + 6$. Then the inequalities (2.11) yield

$$X_j \leqslant \begin{cases} p, & j = 1, 2, 3, \\ p + 1, & j = 4, 5, 6, 7. \end{cases}$$

Thus, $X_1 + X_2 + \cdots + X_7 \leqslant 7p + 4$, a contradiction. If one takes

$$X_j = \begin{cases} p, & j = 1, 2, \\ p + 1, & j > 2, \end{cases}$$

it is easily seen that (2.9) is satisfied, and $X_1 + X_2 + \cdots + X_7 = 7p + 5$.

Note that in each of the above cases the solution given is for the maximal value of t for which the set can contain A_1, A_2, and A_3. For smaller t it is clear from (2.9) that a solution is obtained by simply decreasing the X's of the given solution. ∎

THEOREM 3. *For* $t \geqslant 3$,

$$M_t(t + r, 4) = t + r + 2, \text{ for } f_4(r) \leqslant t \leqslant 4r + 3, \text{ and}$$
$$\geqslant t + r + 3, \text{ for } t < f_4(r),$$

where

$$(2.12)\quad f_4(r) = \begin{cases} 3(r + 2) + \left[\dfrac{(r + 2)}{5}\right], & \text{for } r = 2, 3 \bmod 5, \\ 3r + 5 + \left[\dfrac{(r + 2)}{5}\right], & \text{for } r = 1 \bmod 5, \\ 3r + 4 + \left[\dfrac{(r + 2)}{5}\right], & \text{for } r = 0 \bmod 5, \\ 3(r + 1) + \left[\dfrac{(r + 2)}{5}\right], & \text{for } r = 4 \bmod 5. \end{cases}$$

Proof. The proof is identical to that of Theorem 2. The possible coordinates of A_1, A_2, and A_3, up to multiples, are

(2.13)

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
A_1:	0	0	1	1	1	1	0	1	1	1	1
A_2:	0	1	0	1	α	α^2	1	0	1	α	α^2
A_3:	1	0	0	0	0	0	1	1	1	1	1

	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}	x_{20}	x_{21}
A_1:	0	1	1	1	1	0	1	1	1	1
A_2:	1	0	1	α	α^2	1	0	1	α	α^2
A_3:	α	α	α	α	α	α^2	α^2	α^2	α^2	α^2

Considering all possible linear combinations of the A's yields

$$BX \leqslant D, \tag{2.14}$$

where

$$B = \left[\begin{array}{c|c|c|c|c}
\begin{matrix}1\\1\\1\\1\\1\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&1&1&1\\1&0&1&0&0\\1&1&0&0&0\\1&0&0&1&0\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&1&0&0\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&1&0&0&0\end{matrix} \\ \hline
\begin{matrix}0\\0\\0\\0\\0\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix} & \begin{matrix}0&0&0&0&0\\1&0&1&0&0\\1&1&0&0&0\\1&0&0&0&1\\1&0&0&1&0\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&0&1&0&0\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&1&0&0&0\\1&0&0&1&0\end{matrix} \\ \hline
\begin{matrix}0\\0\\0\\0\\0\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\end{matrix} & \begin{matrix}0&1&1&1&1\\1&0&1&0&0\\0&0&0&1&0\\1&0&0&0&1\\0&1&0&0&0\end{matrix} & \begin{matrix}0&0&0&0&0\\1&0&1&0&0\\1&1&0&0&0\\1&0&0&0&1\\1&0&0&1&0\end{matrix} \\ \hline
\begin{matrix}0\\0\\0\\0\\0\end{matrix} & \begin{matrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&1&0&0&0\\1&0&0&1&0\end{matrix} & \begin{matrix}0&1&1&1&1\\1&0&1&0&0\\1&1&0&0&0\\1&0&0&0&1\\0&1&0&0&0\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\1&0&0&1&0\end{matrix} \\ \hline
\begin{matrix}0\\1\\1\\1\\1\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{matrix} & \begin{matrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{matrix}
\end{array}\right], \quad D = \left[\begin{array}{c}
r \\ r \\ r+1 \\ r+1 \\ r+1 \\ \hline
r+1 \\ r+1 \\ r+2 \\ r+2 \\ r+2 \\ \hline
r+1 \\ r+1 \\ r+2 \\ r+2 \\ r+2 \\ \hline
r+1 \\ r+1 \\ r+2 \\ r+2 \\ r+2 \\ \hline
r
\end{array}\right],$$

and

$$X' = (X_1, X_2, X_3, \ldots, X_{20}, X_{21}).$$

Solutions which correspond to maximal t with the A's in the set are:

$r = 5p$

$$X_j = \begin{cases} p+1, & j = 9, 16, 20, \\ p, & \text{otherwise.} \end{cases}$$

$r = 5p + 1$

$$X_j = \begin{cases} p+1, & j = 4, 7, 8, 10, 11, 14, 15, 19, 21, \\ p-1, & j = 9, \\ p, & j = \text{otherwise.} \end{cases}$$

$r = 5p + 2$

$$X_j = \begin{cases} p, & j = 1, 2, 3, 5, 9, 12, 16, 18, \\ p+1, & \text{otherwise.} \end{cases}$$

$r = 5p + 3$

$$X_j = \begin{cases} p, & j = 1, 2, 3, \\ p+1, & j > 3. \end{cases}$$

$r = 5p + 4$

$$X_j = \begin{cases} p, & j = 1, 2, \\ p+1, & j > 2. \end{cases}$$

One can establish similar results for other values of s. The problem lies in exhibiting a solution to the basic inequalities analogous to (2.14).

References

1. R. C. Bose, Mathematical theory of symmetrical factorial designs, *Sankhyā* **8** (1947), 107–166.
2. R. C. Bose, On some connections between design of experiments and information theory, *Bull. Inst. Int. Statist.* **38** (1961), 257–271.
3. K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Statist.* **23** (1952), 425–434.
4. R. A. Fisher, A system of confounding for factors with more than two alternatives giving completely orthogonal cubes and higher powers, *Ann. Eugenics* **12** (1944), 283–290.
5. R. A. Fisher, The theory of confounding in factorial experiments in relation to theory of groups, *Ann. Eugenics* **12** (1945), 341–353.
6. B. R. Gulati and E. G. Kounias, On bounds useful in the theory of symmetrical factorial designs, *J. Roy. Statist. Soc.* Ser. *B* **32**, No. 1 (1970), 123–133.

7. B. R. GULATI, On the packing problem and its applications (1969), unpublished thesis, University of Connecticut.
8. B. SEGRE, Curve razionale e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* (4) **39** (1955), 357–379.
9. B. SEGRE, "Lectures on Modern Geometry," Cremonese, Roma, 1961.
10. B. SEGRE, Introduction to Galois geometries, *Mem. Accad. Naz. Lincei Ser.* 8 **8** (1967), 133–236.
11. G. TALLINI, Un'applicazione delle geometrie di Galois a questioni di statistica, *Rend. Accad. Naz. Lincei* **35** (1963), 479–485.